



RECEIVED  
DEC 21 2004  
Technology Center 2100



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto  
is a true copy from the records of the Korean Intellectual  
Property Office.

출 원 번 호 : 10-2000-0021151  
Application Number

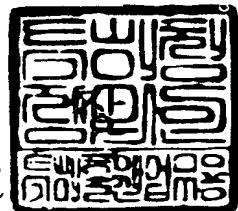
출 원 년 월 일 : 2000년 04월 21일  
Date of Application APR 21, 2000

출 원 인 : 주식회사 플랜티넷  
Applicant(s) PLANTY-NET CO., LTD.

2004 년 10 월 22 일

특 허 청

COMMISSIONER



## 【서지사항】

【서류명】 출원인명의변경신고서  
【수신처】 특허청장  
【제출일자】 2000.08.09  
【구명의인(양도인)】  
    【명칭】 델타넷주식회사  
    【출원인코드】 120000191241  
【신명의인(양수인)】  
    【성명】 주식회사 플랜티넷  
    【출원인코드】 120000374578  
【대리인】  
    【성명】 정상섭  
    【대리인코드】 920000001591  
    【포괄위임등록번호】 20000219035  
【사건의 표시】  
    【출원번호】 1020000021151  
    【출원일자】 2000.04.21  
    【심사청구일자】 2000.04.21  
    【발명의 명칭】 유해사이트의 접속차단 서비스 제공장치 및 방법  
【변경원인】 전부양도  
【취지】 특허법 제38조제4항·실용신안법 제20조·의장법 제24조 및 상표법 제12조제1항의 규정에 의하여 위와 같이 신고합니다.  
【수수료】 13000  
【첨부서류】 양도증 1통 인감증명서 1통

## 【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0003
【제출일자】	2000.04.21
【발명의 명칭】	유해사이트의 접속차단 서비스 제공장치 및 방법
【발명의 영문명칭】	APPARATUS AND METHOD FOR INTERCEPT LINK OF UNWHOLESM SITE IN INTERNET
【출원인】	
【명칭】	델타넷주식회사
【출원인코드】	1-2000-019124-1
【대리인】	
【성명】	손원
【대리인코드】	9-1998-000281-5
【포괄위임등록번호】	2000-021902-8
【대리인】	
【성명】	윤영채
【대리인코드】	9-2000-000158-4
【포괄위임등록번호】	2000-021904-2
【대리인】	
【성명】	정상섭
【대리인코드】	9-2000-000159-1
【포괄위임등록번호】	2000-021903-5
【발명자】	
【성명의 국문표기】	김태주
【성명의 영문표기】	KIM, Tae Ju
【주민등록번호】	620205-1055420
【우편번호】	135-240
【주소】	서울특별시 강남구 개포동 185 주공아파트 705-1101
【국적】	KR
【심사청구】	청구

## 【취지】

특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인  
손원 (인) 대리인  
윤영채 (인) 대리인  
정상섭 (인)

## 【수수료】

【기본출원료】	20	면	29,000	원
【가산출원료】	0	면	0	원
【우선권주장료】	0	건	0	원
【심사청구료】	8	항	365,000	원
【합계】			394,000	원
【감면사유】			소기업 (70%감면)	
【감면후 수수료】			118,200	원
【첨부서류】			1. 요약서·명세서(도면)_1통 2. 소기업임을 증명하는 서류_1통	

**【요약서】****【요약】**

본 발명은 사용자에 의해 노력을 요하는 기존의 수동적인 방식에서 탈피하여 네트워크 제공자가 중앙제어에 의해 가입자의 요청에 따라 유해정보 접근을 차단하도록 하여, 접속차단 관리를 위하여 소요되는 가입자의 시간 및 경비를 절감시키면서 안심하고 인터넷을 이용할 수 있도록 하는 유해 사이트의 접속 차단 서비스 제공 장치 및 방법에 관한 것으로, 본 발명에 따른 장치는 차단대상이 되는 유해 사이트에 대한 제어목록을 현행화하여 제공하며 가입자를 관리하는 중앙제어센터;와, 상기 중앙제어센터와 다수의 원격제어장치를 연결하는 접속제어망;와, 인터넷서비스제공자(ISP)와 가입자 사이에 구비되어 상기 중앙제어센터로부터 제공되는 차단대상 제어목록에 근거하여 가입자의 유해 사이트에 대한 접속시도시 이를 차단하는 다수의 원격제어장치;로 이루어지고, 본 서비스에 가입한 가입자가 소정사이트로의 접속을 시도할 경우, 중앙제어센터에 의해 현행화된 유해사이트목록과 목적지 URL을 비교하여, 가입자가 유해정보사이트로의 접속을 시도하고 있는 것으로 판단되면, 접속불가메시지를 가입자에게 인가하고, 아니라면 고객이 가입한 인터넷서비스제공자에게 접속정보를 제공하여 접속이 이루어지도록 하는 것이다.

**【대표도】**

도 1

**【색인어】**

음란 사이트, 유해 사이트, 중앙제어, 접속 차단, 원격차단,

## 【명세서】

## 【발명의 명칭】

유해사이트의 접속차단 서비스 제공 장치 및 방법{APPARATUS AND METHOD FOR INTERCEPT  
LINK OF UNWHOLESOME SITE IN INTERNET}

## 【도면의 간단한 설명】

도 1은 본 발명에 따른 방법에 따라서 유해정보사이트의 접속을 차단하는 서비스를 제공하는 장치의 전체 개념도이다.

도 2는 본 발명에 따른 유해정보 사이트의 접속 차단 서비스를 제공하는 장치에 있어서 중앙제어센터의 구성을 보이는 블럭도이다.

도 3은 본 발명에 따른 유해정보 사이트의 접속 차단 서비스 제공 장치에 있어서 원격제어장치의 구성을 보이는 블럭도이다.

도 4는 본 발명에 따른 장치를 이용한 유행정보 차단망의 구성예를 보이는 개념도이다.

도 5는 본 발명에 따른 유해 정보 사이트의 접속 차단 서비스를 제공하는 방법을 보이는 플로우챠트이다.

도 6은 유해정보사이트 목록의 현행화 과정을 보이는 플로우챠트이다.

## \*도면의 주요 부분에 대한 부호의 설명\*

10 : 중앙제어센터 20 : 접속제어망

30 : 원격제어장치 40 : 가입자단말기

50 : 인터넷서비스제공자(ISP : Internet Service Provider)

**【발명의 상세한 설명】****【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

<11> 본 발명은 유해한 사이트로 분류되는 특정 인터넷 사이트에 대한 접속을 제한하는 가입자별 인터넷 접속 서비스를 제공하는 유해 사이트의 접속 차단 서비스 제공 장치 및 방법에 관한 것이다.

<12> 현재, 인터넷은 기존의 생활방식과 사고의 패러다임을 바꾸어 놓을 정도로 경이적인 성장을 하고 있는 상황이며, 세계 각국은 지식정보기반 사회의 구축을 기치로 초고속 네트워크의 구축, 다양한 멀티미디어 콘텐츠의 개발, 통신 시장의 경쟁확대 등을 통하여 인터넷 이용의 활성화에 경쟁적으로 나서고 있다.

<13> 이러한, 인터넷은 다양하고 유익한 정보를 제공하여 훌륭한 정보 교류의 장으로서 인식되는 반면에, 각 인터넷 사이트에 접근하는 사용자에 대한 선별기능을 제공하지 않는 개방적인 특성과, 무분별한 사이트의 구축으로 청소년의 음란물 사이트 접속을 비롯한 우려할 만한 인터넷의 역기능적인 측면도 부각되고 있다.

<14> 현재, 유해정보 차단 방식은 사용자의 클라이언트 PC에 유해정보 차단 소프트웨어를 설치하여 사용하거나, 유해정보 시스템을 각 학교나 단체의 LAN에 설치하여 각 LAN별로 접근제어를 행하는 방식으로 이루어지고 있다.

<15> 전자의 경우는 주로 가정에서 사용되는 형태로 청소년들이 음란물, 마약 등 기타 유해정보 사이트에 대한 접속을 제한하기 위해 부모들이 관리해주는 방식이기 때문에, 부모들의 컴퓨터

터 활용 지식이 자녀들보다 떨어지면 실질적인 유해정보 사이트에 대한 차단은 무방비 상태가 된다는 단점이 있다.

<16> 그리고, 후자의 경우는 주로 학교나 단체에서 관리자가 유해정보 차단 서버를 관리되어야 하므로, 시간과 비용의 낭비가 많이 들어, 따로 전담 관리자를 두어야 한다는 단점이 있다.

#### 【발명이 이루고자 하는 기술적 과제】

<17> 본 발명은 상술한 종래의 문제점들을 해결하기 위하여 제안된 것으로서, 그 목적은 사용자에 의해 노력을 요하는 기존의 수동적인 방식에서 탈피하여 네트워크 제공자가 중앙제어에 의해 가입자의 요청에 따라 유해정보 접근을 차단하도록 하는 유해 사이트의 접속 차단 서비스 제공 장치 및 방법을 제공하는 것이다.

<18> 또한, 본 발명의 목적은 유해사이트의 접속 차단 관리를 위하여 소요되는 가입자의 시간 및 경비를 절감시키면서 가입자가 안심하고 인터넷을 이용할 수 있도록 하는 유해 사이트의 접속 차단 서비스 제공 장치 및 방법을 제공하는 것이다.

#### 【발명의 구성】

<19> 상술한 본 발명의 목적을 달성하기 위한 구성수단으로서, 본 발명에 의한 유해사이트의 접속 차단 서비스 제공장치는

<20> 차단대상이 되는 유해 사이트에 대한 제어목록을 현행화하여 제공하며 가입자를 관리하는 중앙제어센터;

<21> 상기 중앙제어센터와 다수의 원격제어장치를 연결하는 접속제어망;

<22> 인터넷서비스제공자(ISP)와 가입자 사이에 구비되어 상기 중앙제어센터로부터 제공되는 차단대상 제어목록에 근거하여 가입자의 유해 사이트에 대한 접속시도시 이를 차단하는 다수의 원격제어장치;

<23> 로 이루어지는 것을 특징으로 한다.

<24> 더하여, 상기와 같이 구성된 유해사이트의 접속차단 서비스제공장치를 이용한 서비스제공방법은

<25> 소정의 인터넷 사용자가 접속차단서비스에 가입하면, 상기 가입자의 정보를 등록한 후 원격제어장치에 제공하는 제1단계;

<26> 등록된 가입자가 인터넷을 통해 소정사이트로의 접속을 시도할 경우, 중앙제어센터에 의해 현행화된 유해사이트목록과 목적지 URL을 비교하여, 가입자가 유해정보 사이트에 접속을 시도하고 있는지를 판단하는 제2단계;

<27> 상기에서 가입자의 접속지가 유해사이트목록내에 포함되면, 유해정보사이트로의 접속을 시도하고 있는 것으로 판단하여, 가입자의 단말기로 접속불가 메시지를 전송하는 제3단계;

<28> 상기에서 가입자의 접속지 URL이 유해사이트 목록내에 포함된 것이 아니라면, 고객이 가입한 인터넷서비스제공자에게 접속정보를 제공하여 접속이 이루어지도록 하는 제4단계;로 이루어지고,

<29> 가입자에 대한 접속시도가 이루어질 때마다 상기 제2단계에서 제4단계 과정이 반복수행 되는 것을 특징으로 한다.

<30> 이하, 첨부한 도면을 참조하여 본 발명에 따른 인터넷에서의 유해정보 사이트의 접속을 차단하는 장치 및 방법의 구성 및 작용에 대하여 상세하게 설명한다.

<31> 도 1은 본 발명에 따른 인터넷에서의 유해정보 사이트의 접속차단시스템을 설명하는 개념도로서, 상기 유해정보사이트의 접속차단 시스템은 차단대상이 되는 유해 사이트에 대한 제어목록을 현행화하여 제공하며 가입자를 관리하는 중앙제어센터(10)와, 상기 중앙제어센터(10)와 원격제어장치(30)를 연결하는 접속제어망(20)과, 인터넷서비스제공자(ISP)와 가입자사이에 구비되어 상기 중앙제어센터(10)로부터 제공되는 차단대상 제어목록에 근거하여 가입자의 유해사이트에 대한 접속시도시 이를 차단하는 원격제어장치(30)와, 유해사이트 접속차단 서비스에 가입하여 원격제어장치(30)를 통해 인터넷접속을 하게 되는 가입자(40)로 이루어진다.

<32> 상기 미설명부호 50은 인터넷접속서비스를 제공하는 인터넷 서비스 제공자(ISP : Internet Service Provider)들이다.

<33> 도 2는 상기 도 1에 도시한 구성수단중, 중앙제어센터(10)의 구성을 보이는 블럭도로서, 차단대상인 유해정보사이트를 실시간으로 검색하여 등록하고, 이등록된 유해정보사이트목록을 접속제어망(20)을 통해 원격제어장치(30)들에 제공하는 중앙제어시스템(11)과, 인터넷이라는 방대한 정보간에서 유해정보사이트를 검색하는 검색시스템(12)과, 상기 검색시스템(12)에 의해 서 추출된 유행정보를 포함하는 인터넷 사이트의 목록을 분류, 등록, 보관, 관리, 변경하는 차단목록시스템(13)으로 구성되며, 상기 검색시스템(12)은 인터넷상에서 제공되는 모든 문서의 정보를 추출하는 웹로봇과 상기 웹로봇이 추출한 콘텐츠의 내용을 체크하여 유행정보의 포함하는 사이트의 목록정보를 추출하는 엑스퍼트엔진으로 이루어져 인터넷에 등록된 사이트의 내용을 자동검색하여 유해정보를 포함하는 사이트를 자동으로 추출해내는 자동검색시스템(12a)과 검색사가 수동으로 유해정보를 포함하는 사이트를 검색하는 수동검색시스템(12b)으로 이루어지고, 차단목록시스템(13)은 차단대상이 되는 유해정보 사이트의 목록을 저장하고 원시 데이터를 수집하여 차단대상 URL별로 등급을 정하고 데이터베이스화하는 데이터베이스(13a)와, 상기 검

색시스템(12)으로부터 보내오는 사이트정보를 기반으로 해당 사이트가 불건전한 유해사이트인지 아닌지를 판단하는 분류시스템(13b)와, 카테고리, 사이트, 등급, 대표단어, 무효사이트 삭제등 상기 등록된 유해사이트목록을 관리하는 관리시스템(13c)으로 이루어진다.

<34> 상기에서, 자동검색시스템(12a)의 웹로봇은 HTTP(Hypertext Transfer Protocol) 프로토콜을 통하여 인터넷상에 있는 모든 문서의 정보를 추출해오는데, 이때 가져오는 정보에 대한 중복성을 조사하여 너무 한 사이트에 깊이 빠지는 현상을 방지한다. 그리고, 자동검색시스템(12a)의 엑스퍼트 엔진은 문자, 그림, 동영상, 채팅, 뉴스그룹 및 FTP 다운로드를 포함하는 유해정보 대상을 추출하여 이들을 포함하는 인터넷 사이트의 목록정보를 추출해 낸다.

<35> 그리고, 수동검색시스템(12b)은 자동검색시스템(12a)에 의해서 찾을 수 없는 유해정보 사이트를 찾아내기 위한 것으로서, 인터넷 전문검색사가 검색엔진을 통해 작업하는 것을 말한다.

<36> 상기와 같은 자동검색시스템(12a) 또는 수동검색시스템(12b)으로부터 출력되는 유해사이트 정보는 차단목록시스템(13)으로 입력되는데, 이때 분류시스템(13b)이 검색시스템(12)에서 보내오는 정보를 기반으로 그 사이트가 불건전한 사이트인지를 판단하는데, 이 판단은 카테고리별로 정해진 임계값(Threshold)에 의해 판단

된다. 이렇게 분류시스템(13b)에 의해 불건전한 사이트로 판단된 유해사이트 목록은 데이터베이스(13)에 저장되는데, 상기 데이터베이스(13)는 최초에 차단대상 URL 목록검색작업을 통하여 원시데이터를 수집하여 차단대상 URL에 대한 등급을 정한 후 데이터베이스화한다. 그리고, 이렇게 데이터베이스(13)에 보관된 유해정보사이트의 목록을 상기 관리시스템(13c)은 카테고리, 사이트, 등급, 대표단어의 변경, 무효사이트 삭제등을 수행하여 관리한다. 이때, 카테고리는 추가, 수정, 삭제할 수 있어야 하며, 분류시스템(13b)으로부터 불건전 사이트로 판정받은 사이트들을 수정, 삭제할 수 있으며, 신규사이트도 등록할 수 있다. 또한, 이미 구축된 목록중에서 도 무효사이트를 찾아 삭제하게 되어 있다. 여기에는, 가입자로부터의 요청에 따른 해당 URL의 차단대상여부를 재심의하는 과정이 포함된다.

<37> 이에 의하여 본 발명에 따른 유해정보 사이트의 접속차단시스템은 유해정보사이트의 효율적인 탐색, 주기적인 목록 갱신등의 작업을 자동화할 수 있다.

<38> 도 3은 상기 중앙제어센터(10)로부터 보내진 유해정보 사이트 목록을 받아 가입자가 해당 목록에 포함된 사이트에 접속하려 할 시 이를 차단하는 원격제어장치(20)의 구성도로서, 상기 원격제어장치(20)는 중앙제어센터(10)와 연결되어 차단목록을 현행화시키고 이에 따라 가입자의 인터넷접속을 제어하는 차단제어서버(31)와, 상기 중앙제어센터(10)로부터 받은 유해정보 사이트의 목록을 보관하는 접속차단목록DB(32)와, 가입자의 정보이용형태를 분석하여 차단대상 정보인 경우 이를 중앙제어센터(10)로 전달하는 엑스퍼트엔진(33)으로 구성된다.

<39> 상기 차단제어서버(31)내에서는 모니터링시스템(31a)을 포함하고, 중앙제어

센터(10)와 연결되어, 접속차단목록DB(32)를 현행화시키고, 상기 목록에 근거하여 접속차단 서비스에 가입한 가입자의 인터넷 접속제어를 행하여, 해당 ISP(50)로의 접속을 행할지를 결정하여, 차단대상이 아니면 접속을 행한다. 그리고, 별도로 엑스퍼트엔진(33)은 가입자가 접속하는 사이트의 정보를 검색하여 차단대상 정보검색의 경우, 이를 중앙제어센터(10)에 알린다.

<40> 이상 설명한 바와 같이, 구성된 유해정보 사이트 접속차단장치를 적용하면 도 4와 같은 유해정보차단망이 구축된다.

<41> 도 4에서, 유해정보차단망은 각 가정에 구비되는 개인의 퍼스널컴퓨터 또는 소정 단체, 예를 들어, 학교 또는 기업에 구축된 LAN이 해당되는 가입자는 우선 PSTN/ISDN 또는 xDSL 또는 무선망 또는 광동축케이블등과 같은 액세스망을 통해 액세스서버()에 접속되고, 상기 액세스서버는 유해정보차단망, 즉 본 발명에 의한 접속차단장치의 원격제어장치(30)가 구비된 접속제어망(20)을 통해 인터넷접속서비스를 제공하는 인터넷서비스제공자(ISP)에 접속된다.

<42> 따라서, 모든 인터넷사이트에 대한 검색을 실시하여 유해사이트 목록을 현행화시키는 중앙제어센터의 유해사이트정보에 따라서, 가입자의 소정 사이트접속요청중 상기 중앙제어센터에서 제공하는 유해사이트 목록에 포함된 사이트에 대한 접속요청은 차단하고, 상기 유해사이트 목록에 포함되지 않은 접속요청은 인터넷서비스제공자(ISP)에 전달하여 해당 사이트에 대한 접속이 이루어지도록 한다.

<43> 도 5는 본 발명과 같은 유해정보사이트 접속차단시스템을 이용한 유해정보사이트 접속차단서비스 제공방법에 대한 플로우챠트이다.

<44> 상기 도 5에 나타난 바와 같이, 개인 또는 단체(회사 또는 기업등)등에서 먼저 상기와 같은 장치에 의하여 제공되는 유해사이트 접속차단서비스에 가입을 하면(S501), 가입자의 정보

가 중앙제어센터(10)에 등록되고(S502), 중앙제어센터(10)는 등록된 고객정보를 원격제어장치(30)에 제공한다.

<45> 상기와 같이 가입자의 등록과정(S501~S503)이 완료된 후, 본 서비스에 가입한 가입자가 자신의 단말기를 통해 접속을 시도하면(S504), 상기 접속은 도 4에 도시한 액세스서버를 통하여, 원격제어장치(30) 및 접속제어망(20)으로 이루어진 유해정보차단망까지 연결된다(S505).

<46> 이렇게 가입자가 접속을 시도하면, 상기 원격제어장치(30)는 접속자가 본 서비스의 가입자인지를 파악한 후 중앙제어센터(10)에 의해서 현행화된 유해사이트목록과 목적지 URL을 비교하여, 가입자가 유해정보 사이트에 접속을 시도하고 있는지를 판단한다(S506).

<47> 상기에서 가입자의 접속지 URL이 유해사이트목록내에 포함된 것이라면, 유해정보사이트로의 접속을 시도하고 있는 것으로 판단하여, 가입자의 단말기로 접속불가 메시지를 전송한 후 로그파일에 저장한다(S507).

<48> 반대로, 상기에서 가입자의 접속지 URL이 유해사이트 목록내에 포함된 것이 아니라면, 고객이 가입한 인터넷서비스제공자(50)에게 접속정보를 제공하여 접속이 이루어지도록 한다(S508). 이렇게 접속이 이루어지면 가입자는 해당 사이트의 인터넷서핑을 실시한다(S509).

<49> 가입자가 URL 주소를 변경할 때마다 상기 단계 S506~S509는 반복실시되어, 가입자가 유해한 사이트에 접속하는 것을 방지한다.

<50> 상기에서, 가입자에 대한 유해사이트의 접속차단을 보다 신뢰성있게 제공하려면, 유해사이트 목록에 대한 현행화가 이루어져야 한다.

<51> 본 발명에 따른 인터넷에서의 유해정보 사이트의 접속차단시스템에서 이루어지는 유해사이트 목록의 현행화과정을 도 6에 도시한다.

<52> 상기 도 6의 플로우챠트를 참조하면, 중앙제어센터(10)는 초기제어목록DB를 작성한다(S601).

<53> 그 다음, 제어목록을 자동검색시스템(12a)에 의한 자동검색, 수동검색시스템(12b)에 의한 수동검색을 통해 제어목록의 유해정보포함 여부를 검색한다(S602). 그리고, 그 검색결과에 따라서, 차단대상 제어목록을 유해사이트와 유해하지 않은 사이트, 또는 유해정도의 등급별로 분류하고(S603), 상기 검색결과 및 분류결과에 따라서 변경된 내용을 바꿔 제어목록DB의 갱신하고(S604). 또 제어목록의 유효성을 검사하여(S605), 유효하지 않은 사이트는 삭제하는 등의 제어목록DB갱신을 실행하는 과정(S606)을 반복하여, 차단대상 제어목록을 현행화시킨다.

<54> 이상 설명한 인터넷에서의 유해정보 사이트의 접속을 차단하는 장치 및 방법은 중앙제어에 의하여 유해정보사이트에 대한 접속을 차단하는 서비스를 네트워크 측면에서 부가서비스의 형태로 제공함으로써, 가정과 학교에서 청소년들의 불건전한 정보에 대한 접근을 효과적으로 차단하여, 인터넷이 교육을 위한 건전한 지식창고로 활용될 수 있도록 할 수 있고, 직장에서는 증권거래등 업무와 관련없는 용도로 인터넷이 활용되는 것을 제한함으로서 고용인에 대한 관리를 할 수도 있다.

### 【발명의 효과】

<55> 상술한 바와 같이, 본 발명은 가정이나 학교 또는 직장등에서 개별적인 인터넷 접속관리를 할 필요없이 원하지 않는 정보를 제공하는 사이트로의 접근을 효과적으로 차단할 수 있으며, 이로써, 개별적으로 인터넷 접속을 관리하고, 통제를 행하기 위한 시간 및 인력의 낭비를 줄일 수 있어 비용을 절감시킬 수 있으며, 또한, 중앙제어에 의해 원하지 않는 유해사이

102000021151

출력 일자: 2004/10/22

트로의 접근을 차단함으로서 부모나 기업주의 입장에서 안심하고 인터넷을 사용하도록 할 수 있어 인터넷이 보다 건설적이고 교육적으로 이용될 수 있도록 하는 효과가 있다.

**【특허청구범위】****【청구항 1】**

차단대상이 되는 유해 사이트에 대한 제어목록을 현행화하여 제공하며 가입자를 관리하는 중앙제어센터;

상기 중앙제어센터와 다수의 원격제어장치를 연결하는 접속제어망;

인터넷서비스제공자(ISP)와 가입자 사이에 구비되어 상기 중앙제어센터로부터 제공되는 차단대상 제어목록에 근거하여 가입자의 유해 사이트에 대한 접속시도시 이를 차단하는 다수의 원격제어장치;

로 이루어지는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 장치.

**【청구항 2】**

제 1 항에 있어서, 상기 중앙제어센터는

차단대상인 유해정보사이트를 실시간으로 검색하여 등록하고, 이등록된 유해정보사이트 목록을 원격제어장치들에 제공하는 중앙제어시스템;

유해정보사이트를 검색하는 검색시스템;

상기 검색시스템에 의해서 추출된 유행정보를 포함하는 인터넷 사이트의 목록을 분류, 등록, 보관, 관리, 변경하는 차단목록시스템;

으로 이루어지는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 장치.

**【청구항 3】**

제 2 항에 있어서, 상기 검색시스템은

인터넷상에서 제공되는 모든 문서의 정보를 추출하는 웹로봇과 상기 웹로봇이 추출한 콘텐츠의 내용을 체크하여 유행정보의 포함하는 사이트의 목록정보를 추출하는 엑스퍼트엔진으로 이루어져 인터넷에 등록된 사이트의 내용을 자동검색하여 유해정보를 포함하는 사이트를 자동으로 추출해내는 자동검색시스템과,

인터넷 전문 검색사가 수동으로 유해정보를 포함하는 사이트를 검색하는 수동검색시스템으로 이루어지는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 장치.

**【청구항 4】**

제 2 항에 있어서, 상기 차단목록시스템은

차단대상이 되는 유해정보 사이트의 목록을 저장하고 원시 데이터를 수집하여 차단대상 URL별로 등급을 정하고 데이터베이스화하는 데이터베이스;

상기 검색시스템으로부터 보내오는 사이트정보를 기반으로 해당 사이트가 불건전한 유해 사이트인지 아닌지를 판단하는 분류시스템;

카테고리, 사이트, 등급, 대표단어, 무효사이트 삭제등 상기 등록된 유해사이트목록을 관리하는 관리시스템;

으로 이루어지는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 장치.

**【청구항 5】**

제 3 항에 있어서, 자동검색시스템의 웹로봇은 인터넷상에 있는 모든 문서의 정보를 추출해오는데, 이때 가져오는 정보에 대한 중복성을 조사하여 너무 한 사이트에 깊이 빠지는 현상을 방지하는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 장치.

**【청구항 6】**

제 1 항에 있어서, 상기 원격제어장치는  
중앙제어센터와 연결되어 차단목록을 현행화시키고 이에 따라 가입자의 인터넷접속을  
제어하는 차단제어서버;

상기 중앙제어센터로부터 받은 유해정보사이트의 목록을 보관하는 접속차단목록DB;  
가입자의 정보이용형태를 분석하여 차단대상정보인 경우 이를 중앙제어센터로 전달하는  
엑스퍼트엔진;  
으로 구성되는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 장치.

**【청구항 7】**

중앙제어를 통해 가입자가 유해한 사이트로의 접속시도시 이를 차단하는 유해 사이트의  
접속 차단 서비스 제공 방법에 있어서,

소정의 인터넷 사용자가 접속차단서비스에 가입하면, 상기 가입자의 정보를 등록한 후  
원격제어장치에 제공하는 제1단계;

등록된 가입자가 인터넷을 통해 소정사이트로의 접속을 시도할 경우, 중앙제어센터에 의해  
현행화된 유해사이트목록과 목적지 URL을 비교하여, 가입자가 유해정보 사이트에 접속을 시  
도하고 있는지를 판단하는 제2단계;

상기에서 가입자의 접속지가 유해사이트목록내에 포함되면, 유해정보사이트로의 접속을 시도하고 있는 것으로 판단하여, 가입자의 단말기로 접속불가 메시지를 전송하는 제3단계;

상기에서 가입자의 접속지 URL이 유해사이트 목록내에 포함된 것이 아니라면, 고객이 가입한 인터넷서비스제공자에게 접속정보를 제공하여 접속이 이루어지도록 하는 제4단계;로 이루어지고,

가입자에 대한 접속시도가 이루어질 때마다 상기 제2단계에서 제4단계 과정이 반복수행 되는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 방법.

#### 【청구항 8】

제 7 항에 있어서, 상기 유해 사이트의 접속차단 서비스제공방법은

초기제어목록 DB를 작성하는 제1단계;

제어목록을 유해정보포함 여부를 검색하여, 분류하는 제2단계;

상기 검색결과 및 분류결과에 따라서 변경된 내용을 바꿔 제어목록DB의 갱신하는 제3단계;

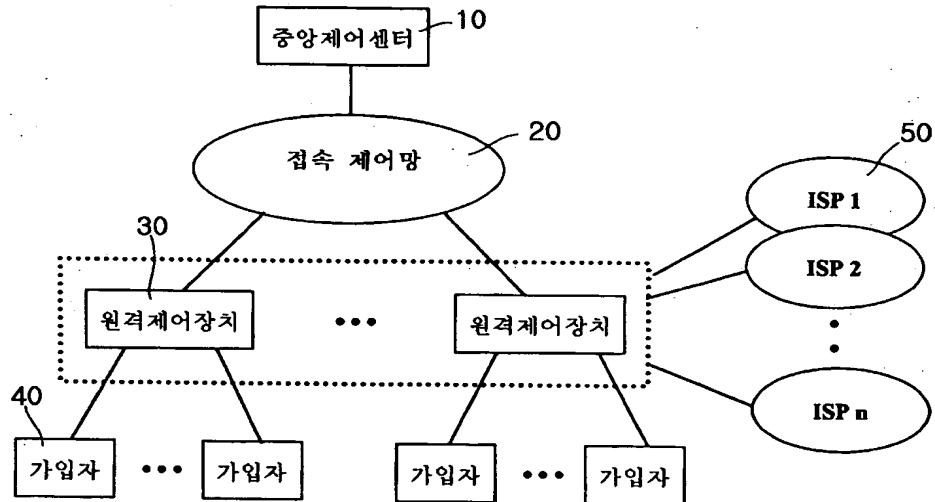
제어목록에 대해 각 사이트의 유효성을 검사하는 제4단계;

유효하지 않은 사이트는 삭제하는 등의 제어목록DB를 갱신하는 제5단계;로 이루어져,

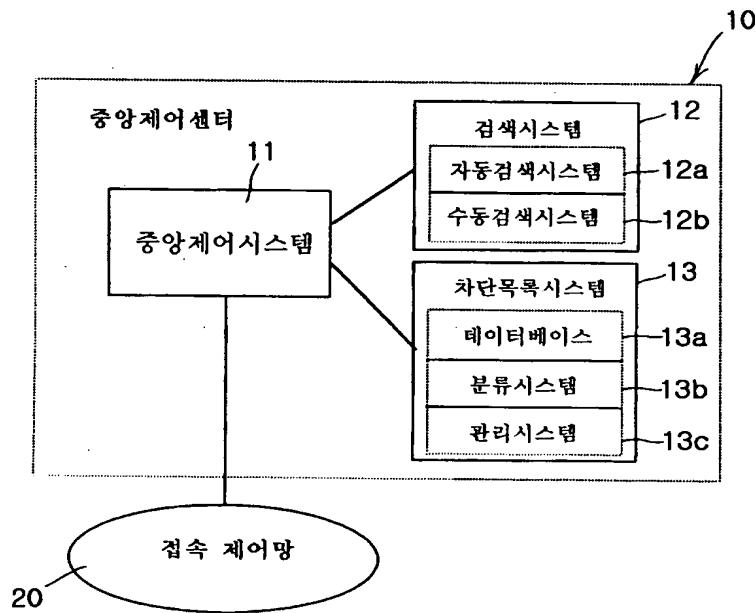
초기제어목록작성후 제2단계에서 제5단계의 과정을 반복수행하여 제어목록을 현행화시키는 것을 특징으로 하는 유해 사이트의 접속 차단 서비스 제공 방법.

## 【도면】

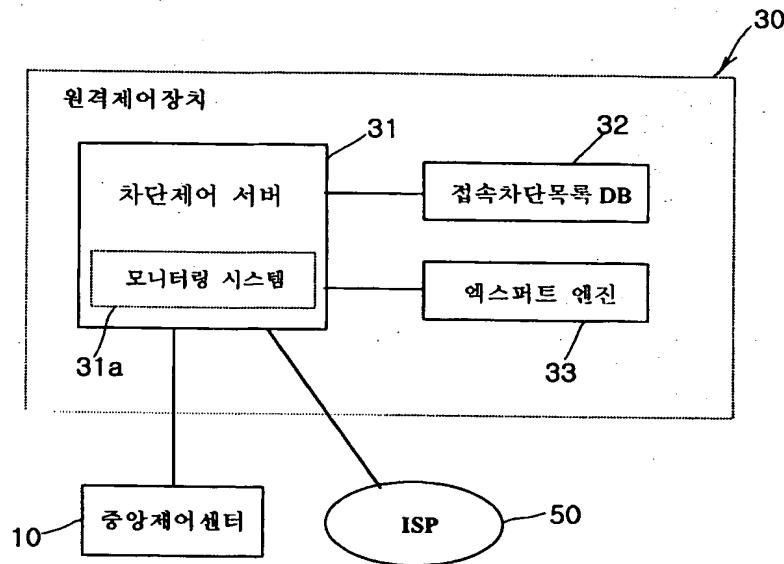
【도 1】



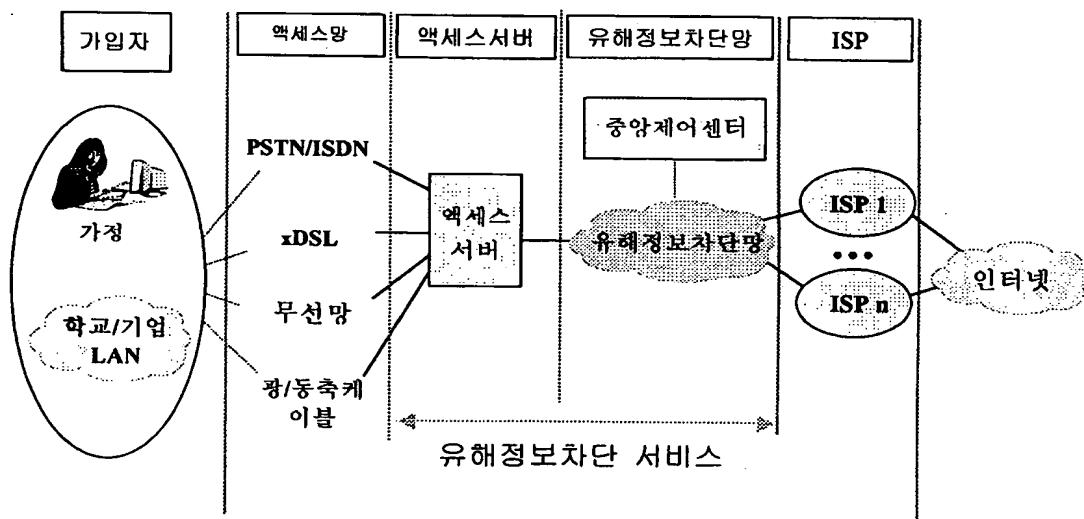
【도 2】



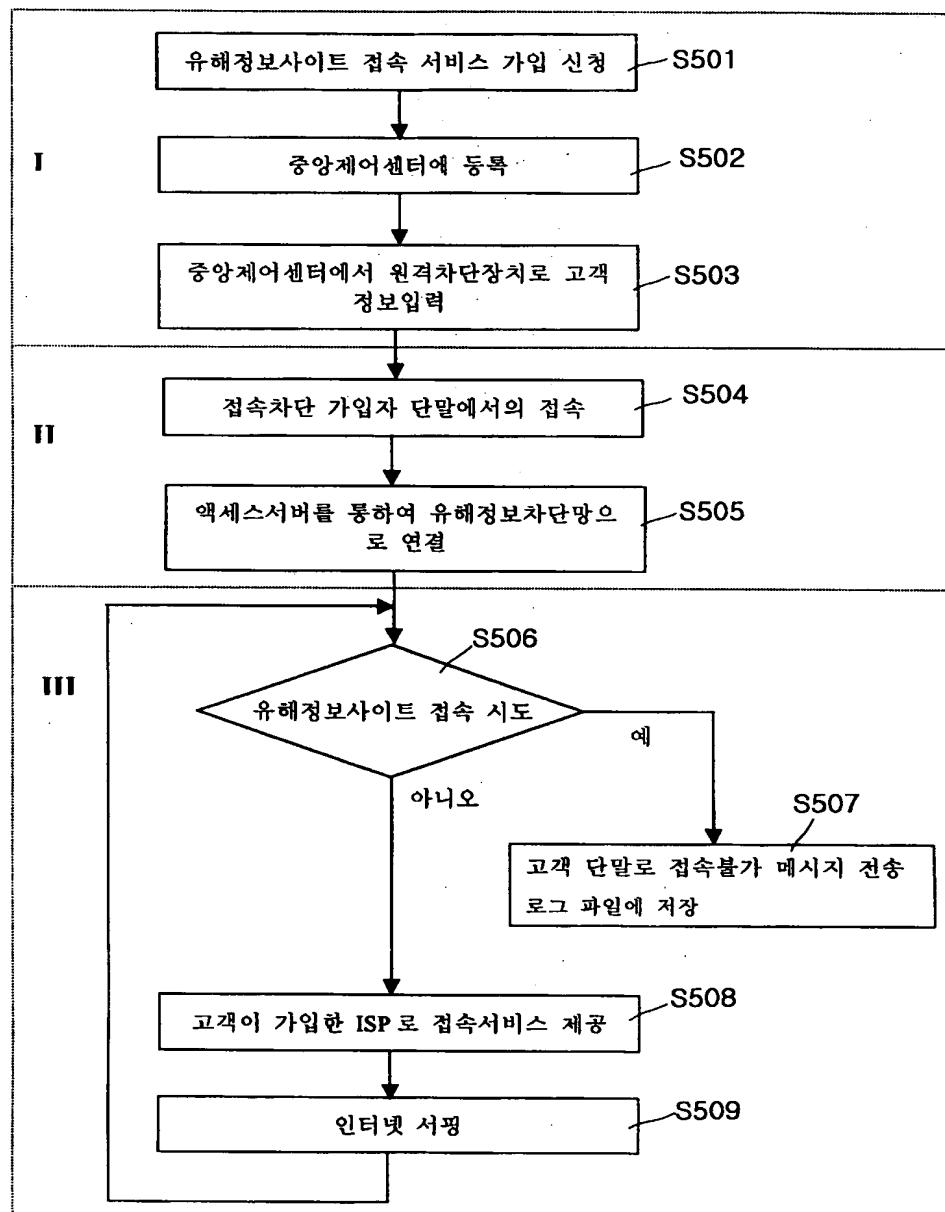
【도 3】



【도 4】



## 【도 5】



【도 6】

